**Name** : Vaibhav Soni

**Enrolment No.** : IU2141230287

**Branch** : CSE – A

**Sem** : 7

**Subject** : Cyber Security

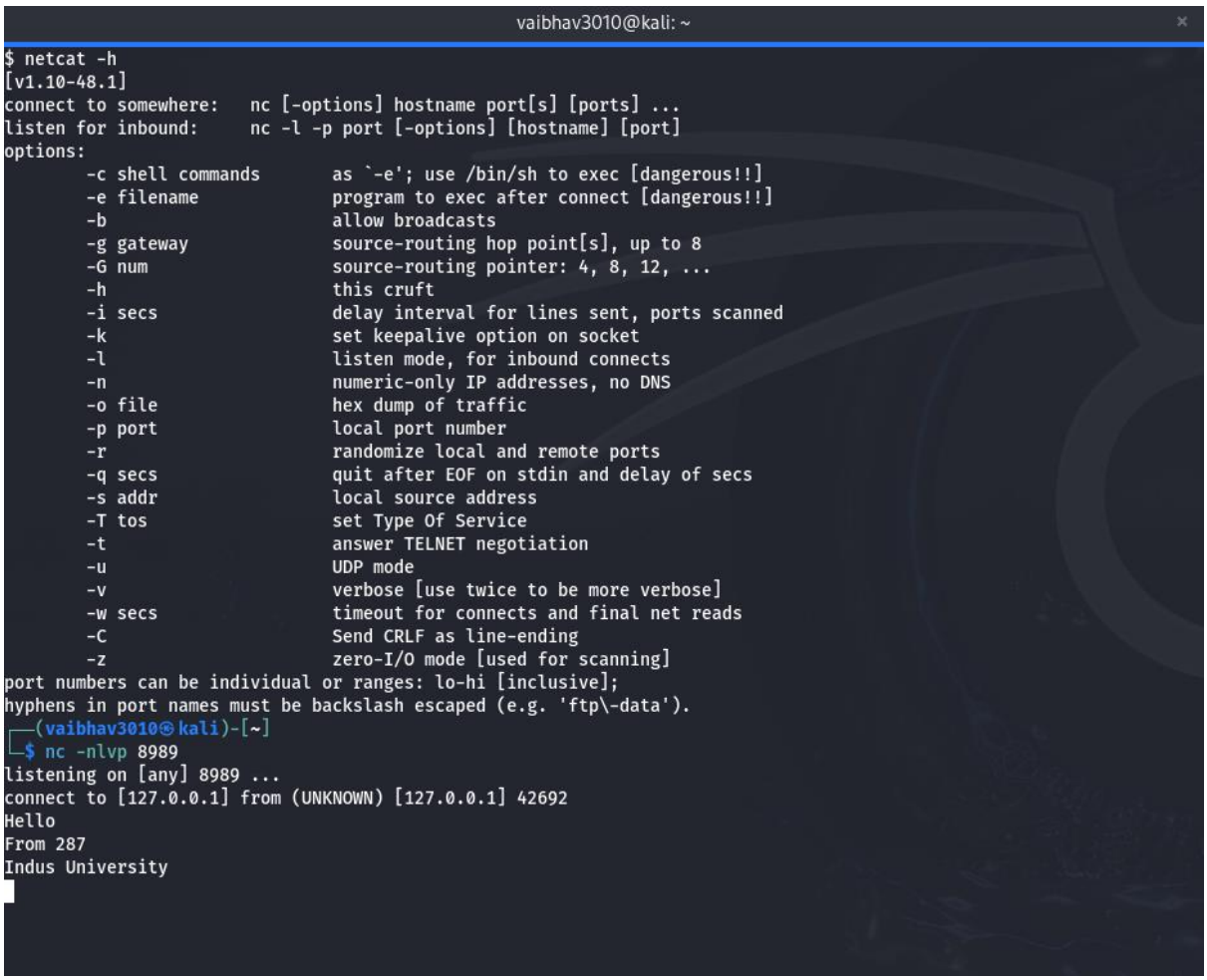
# Lab – 3

**Aim :** TCP / UDP connectivity using Netcat.

**TCP Server Input :**

nc -nlvp 8989

**TCP Server Output :**



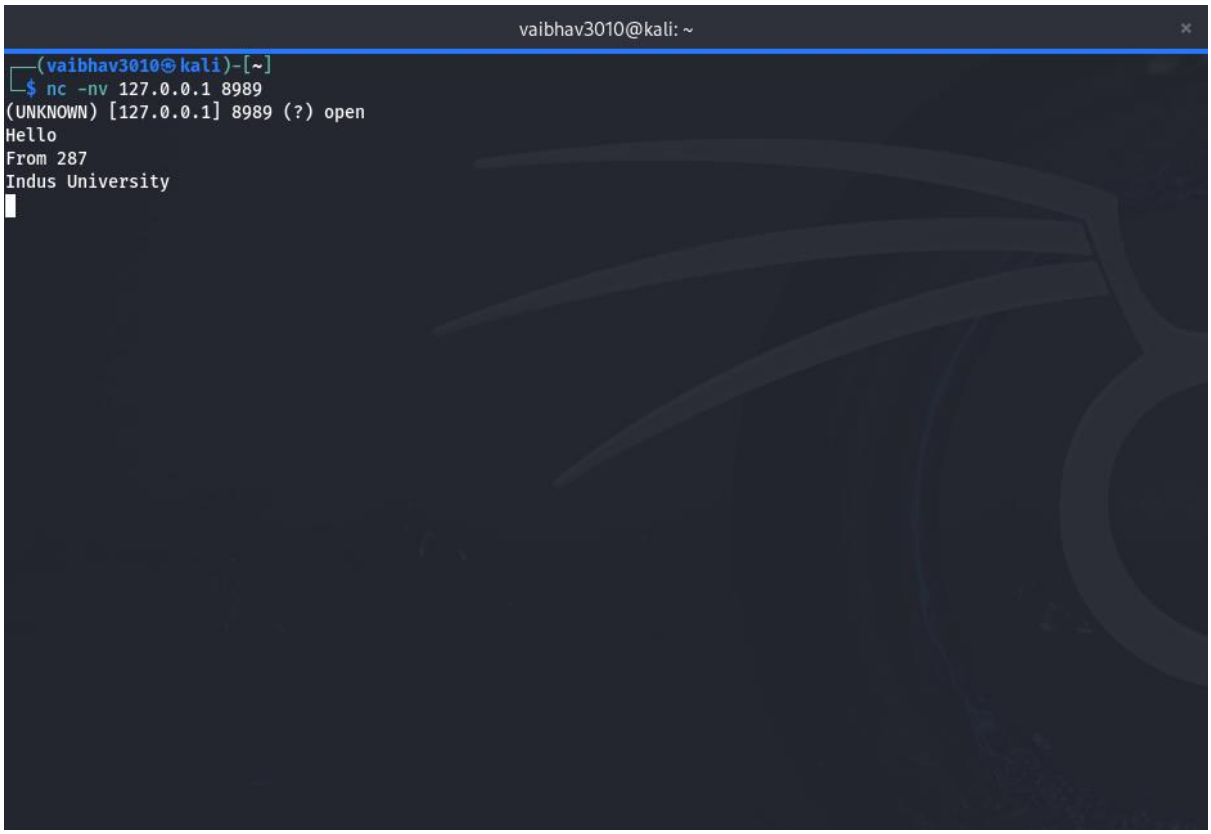
```
vaibhav3010@kali: ~
$ netcat -h
[v1.10-48.1]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
┌──(vaibhav3010㉿kali)-[~]
└─$ nc -nlvp 8989
listening on [any] 8989 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 42692
Hello
From 287
Indus University
```

- The command `nc -nlvp 8989` uses Netcat (`nc`) to listen on port 8989. The options are: `-n` to avoid DNS lookups, `-l` to enable listening mode, `-v` for verbose output, and `-p 8989` to specify the port number. This command is commonly used to set up a simple TCP server for testing and debugging network connections.

**TCP Client Input :**

nc -nv 127.0.0.1 8989

**TCP Client Output :**

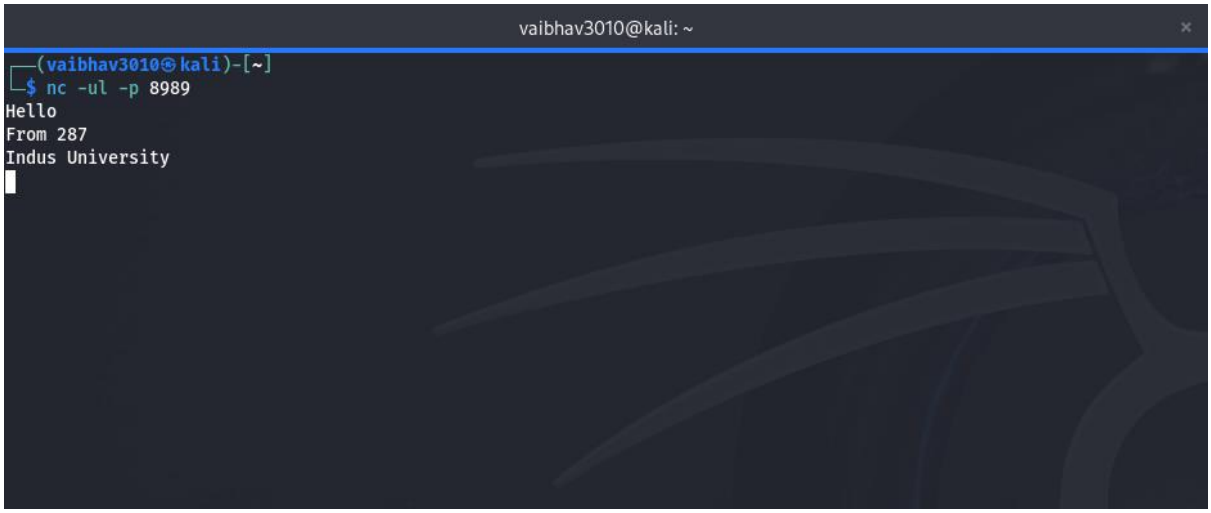



- The command `nc -nv 127.0.0.1 8989` uses Netcat (`nc`) to establish a connection to the IP address 127.0.0.1 (localhost) on port 8989. The `-n` option avoids DNS lookups, and the `-v` option makes the output more verbose. This is often used to test connectivity to a specific port on the local machine.

**UDP Server Input :**

nc -ul -p 8989

**UDP Server Output :**

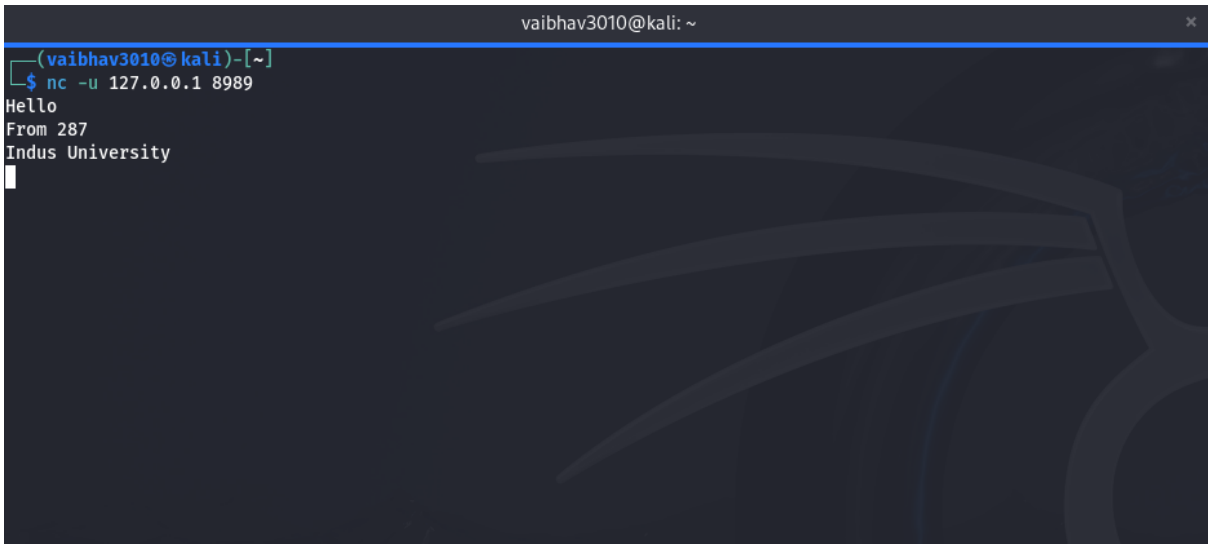



- The command `nc -ul -p 8989` uses Netcat (`nc`) to listen for UDP packets on port 8989. The options `-u` specifies UDP mode, `-l` tells Netcat to listen for incoming connections, and `-p 8989` designates the port number to listen on. This setup is often used for testing UDP communication and for creating simple UDP servers.

**UDP Client Input :**

nc -u 127.0.0.1 8989

**UDP Client Output :**




- The command `nc -u 127.0.0.1 8989` uses Netcat (`nc`) to send data to the IP address 127.0.0.1 (localhost) on port 8989 using the UDP protocol (`-u`). This command is often used for testing UDP communication between hosts.